Exhibit 1

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of New Jersey

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
THE REAL PROPERTY AND RESIDENCE AT [redacted], NEW JERSEY; 2016 BLACK MERCEDES-BENZ C300 BEARING [redacted] 2021 WHITE MERCEDES-BENZ GLE BEARING [redacted] and THE PERSON OF OLUWASEUN ADEKOYA

Case No. 23-16155, 23-16156, 23-16157, 23-16158

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of New Jersey
(identify the person or describe the property to be searched and give its location):

See Attachments A-1, A-2, A-3, and A-4

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachments B-1, B-2, B-3, and B-4

YOU ARE COMMANDED to execute this warrant on or before December 22, 2023 *(not to exceed 14 days)*
❒ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. José R. Almonte.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☑ for 30 days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 12/08/2023 @ 4:02 PM

Jose R. Almonte
Judge's signature

City and state: District of New Jersey

Hon. José R. Almonte
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

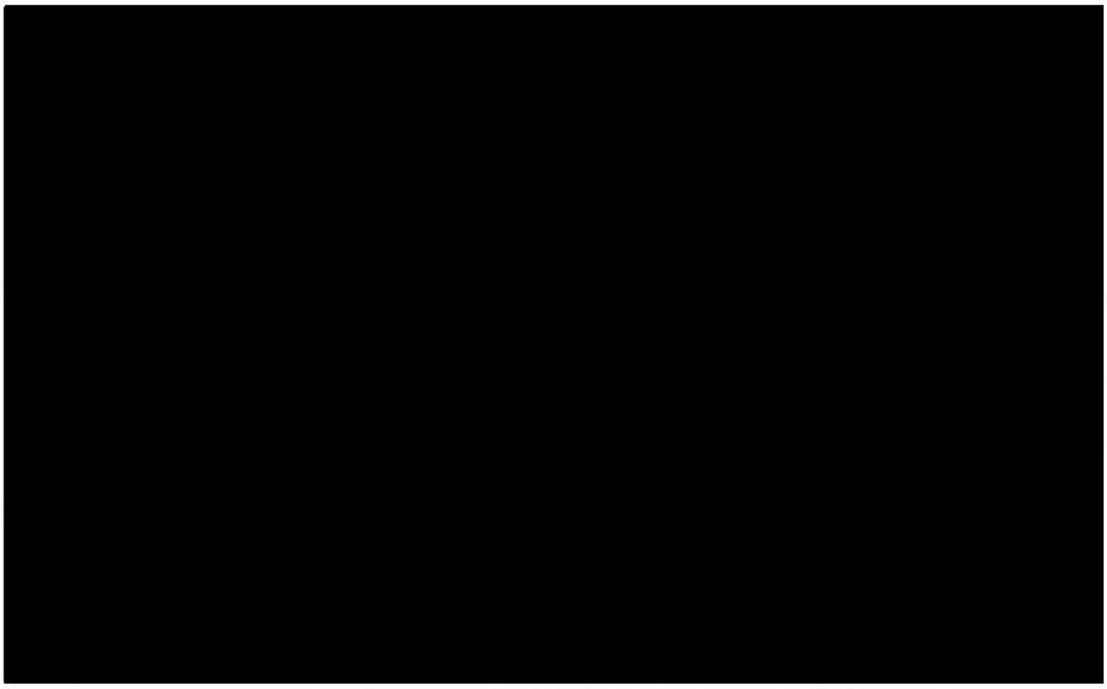
_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-1

Property to be Searched

1. The property to be searched is [redacted] New Jersey 07010 [redacted] and includes any garage space or storage unit under the control of or used by Oluwaseun ADEKOYA at [redacted], New Jersey 07010 and any open or closed containers therein. [redacted] is located within [redacted], which is a high-rise luxury apartment rental community that offers approximately 314 separate studio, one, and two bedroom apartments for lease. The building appears to be approximately 15 stories tall with 24-hour security, a rooftop pool, a grand plaza with restaurants and retail stores, a fitness center, a lounge, and an underground parking garage, per the property's website. Based on publicly accessible floor plans, [redacted] likely contains a living room, a kitchen, a laundry room, closet space, at least one bedroom, and at least one bathroom. A photograph of [redacted]



ATTACHMENT B-1

Items to be Seized

1. All evidence, fruits, and instrumentalities of the crimes of conspiracy to commit bank fraud, in violation of 18 U.S.C. §§ 1349 and 1344 and aggravated identity theft, in violation of 18 U.S.C. § 1028A (aggravated identity theft) (the "Subject Offenses"), involving Oluwaseun ADEKOYA, and any co-conspirators known and unknown, covering the time period of January 1, 2021 to present unless otherwise indicated, including:

a. Evidence concerning occupancy or ownership of [redacted] New Jersey 07010, a 2016 black Mercedes-Benz C300 bearing [redacted], and a 2021 white Mercedes-Benz GLE bearing [redacted] including utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, invoices, registration documents, identification documents, address books, and telephone directories.

b. Evidence concerning aliases or identities used by Oluwaseun ADEKOYA, including identification instruments and documents, financial records, telephone bills, legal records, and other documentation indicating the use by ADEKOYA of a name or identity other than ADEKOYA.

c. Evidence concerning the identity or location of, and communications with, suspects, coconspirators, and bank fraud or identity theft victims.

d. Records related to personal identifying information ("PII") of anyone other than ADEKOYA or his spouse, A[redacted] T[redacted] O[redacted]

e. Records related to credit unions or banks, to include locations, account numbers, participation in shared branching, shared branching transaction limitations.

f. Records related to fraudulent banking transactions conducted in the name of customers, including location information, branch information, transaction amounts, identity of individuals conducting the transactions or in whose name the transactions were conducted, and time and date of transaction.

g. Any and all financial and wealth information for ADEKOYA, including but not limited to bank account records, bank statements, deposit slips, ATM withdrawal slips, cancelled checks, check registers, withdrawal slips, wire and inter-account transfers, cryptocurrency transfers, cashier's checks, money orders, signature cards, mutual fund and other securities records, credit applications, loan documents and loan payments records, debit cards, credit cards, credit card statements, credit card account applications, invoices, vendor

payments, subcontractor invoices, insurance records, deeds, titles, receipts and/or bills evidencing cash expenditures.

h. Records related to the acquisition or purchase of customer financial information, PII, and fake identifications.

i. Evidence of the disposition of proceeds of the Subject Offenses, including U.S. currency, foreign currency, cryptocurrency, jewelry, precious metals, other valuables, pre-paid debit cards, financial instruments, and financial accounts constituting or traceable to the proceeds of the Subject Offenses, and including any passwords, passphrases, public or private keys, physical devices, physical keys, and cryptocurrency recover mnemonics needed by law enforcement to access such items.

j. Records and communications relating to the storage of items, records or documents at any other location, including but not limited to contracts and lease agreements for offices, storage units or safe deposit boxes. Keys and other access devices for storage units, safe deposit boxes, vehicles, and other closed containers.

k. Photographs and communications related to the crimes under investigation and identifying victims, coconspirators, or other evidence of criminal activity.

2. The items to be seized include any computer devices, cellular phones, and storage media reasonably believed to contain any electronically

stored information falling within the categories set forth in this Attachment B-1, above. The electronic devices to be seized are limited to desktop computers, laptop computers, tablets, and external storage media ("SHARED COMPUTER EQUIPMENT") found in common areas of [redacted] reasonably believed to be used, possessed, or accessed by ADEKOYA, and SHARED COMPUTER EQUIPMENT and cellular phones: (1) found on the person of, or within reasonable proximity of ADEKOYA; (2) found within a bedroom where ADEKOYA is determined to have been sleeping; (3) attributed to ADEKOYA using biometric unlocking information described below; (4) identified as belonging to ADEKOYA if a law enforcement agent observes an electronic device to ring, vibrate or otherwise indicate receipt of an incoming call when called by a law enforcement agent; (5) identified by ADEKOYA or A[redacted]O[redacted]as belonging to ADEKOYA; or (6) which ADEKOYA or A[redacted]A[redacted] are able to identify as belonging to any specific member of the household.

3. For any computer or storage medium, to include desktop and laptop computers, tablets, disk drives, modems, thumb drives, personal digital assistants, cellular phones, digital cameras, and scanners, whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration

files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

5. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

6. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

7. During the execution of the search, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of ADEKOYA to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face of ADEKOYA and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

8. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT A-2

Property to be Searched

1. The property to be searched is a 2016 black Mercedes-Benz C300 bearing [redacted] (the "C300").

ATTACHMENT B-2

Items to be Seized

1. All evidence, fruits, and instrumentalities of the crimes of conspiracy to commit bank fraud, in violation of 18 U.S.C. §§ 1349 and 1344 and aggravated identity theft, in violation of 18 U.S.C. § 1028A (aggravated identity theft) (the "Subject Offenses"), involving Oluwaseun ADEKOYA, and any co-conspirators known and unknown, covering the time period of January 1, 2021 to present unless otherwise indicated, including:

a. Evidence concerning occupancy or ownership of [redacted], New Jersey 07010, a 2016 black Mercedes-Benz C300 bearing [redacted], and a 2021 white Mercedes-Benz GLE bearing [redacted], including utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, invoices, registration documents, identification documents, address books, and telephone directories.

b. Evidence concerning aliases or identities used by Oluwaseun ADEKOYA, including identification instruments and documents, financial records, telephone bills, legal records, and other documentation indicating the use by ADEKOYA of a name or identity other than ADEKOYA.

c. Evidence concerning the identity or location of, and communications with, suspects, coconspirators, and bank fraud or identity theft victims.

d. Records related to personal identifying information ("PII") of anyone other than ADEKOYA or his spouse, A[redacted] T[redacted] O[redacted]

e. Records related to credit unions or banks, to include locations, account numbers, participation in shared branching, shared branching transaction limitations.

f. Records related to fraudulent banking transactions conducted in the name of customers, including location information, branch information, transaction amounts, identity of individuals conducting the transactions or in whose name the transactions were conducted, and time and date of transaction.

g. Any and all financial and wealth information for ADEKOYA, including but not limited to bank account records, bank statements, deposit slips, ATM withdrawal slips, cancelled checks, check registers, withdrawal slips, wire and inter-account transfers, cryptocurrency transfers, cashier's checks, money orders, signature cards, mutual fund and other securities records, credit applications, loan documents and loan payments records, debit cards, credit cards, credit card statements, credit card account applications, invoices, vendor

payments, subcontractor invoices, insurance records, deeds, titles, receipts and/or bills evidencing cash expenditures.

h. Records related to the acquisition or purchase of customer financial information, PII, and fake identifications.

i. Evidence of the disposition of proceeds of the Subject Offenses, including U.S. currency, foreign currency, cryptocurrency, jewelry, precious metals, other valuables, pre-paid debit cards, financial instruments, and financial accounts constituting or traceable to the proceeds of the Subject Offenses, and including any passwords, passphrases, public or private keys, physical devices, physical keys, and cryptocurrency recover mnemonics needed by law enforcement to access such items.

j. Records and communications relating to the storage of items, records or documents at any other location, including but not limited to contracts and lease agreements for offices, storage units or safe deposit boxes. Keys and other access devices for storage units, safe deposit boxes, vehicles, and other closed containers.

k. Photographs and communications related to the crimes under investigation and identifying victims, coconspirators, or other evidence of criminal activity.

2. The items to be seized include any computer devices, cellular phones, and storage media reasonably believed to contain any electronically

stored information falling within the categories set forth in this Attachment B-2 above, including, but not limited to, desktop and laptop computers, tablets, disk drives, thumb drives, personal digital assistants, cellular phones, digital cameras, and portable scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review. The items to be seized include any cellular telephones that belong to ADEKOYA or are reasonably believed to have been used by ADEKOYA in connection with the Subject Offenses.

3. For any computer or storage medium, to include desktop and laptop computers, tablets, disk drives, modems, thumb drives, personal digital assistants, cellular phones, digital cameras, and scanners, whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or

absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and

cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

5. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

6. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

7. During the execution of the search, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of ADEKOYA to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face of ADEKOYA and activate the facial recognition feature, for the

purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

8. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT A-3

Property to be Searched

1. The property to be searched is a 2021 white Mercedes-Benz GLE bearing [redacted]

ATTACHMENT B-3

Items to be Seized

1. All evidence, fruits, and instrumentalities of the crimes of conspiracy to commit bank fraud, in violation of 18 U.S.C. §§ 1349 and 1344 and aggravated identity theft, in violation of 18 U.S.C. § 1028A (aggravated identity theft) (the "Subject Offenses"), involving Oluwaseun ADEKOYA, and any co-conspirators known and unknown, covering the time period of January 1, 2021 to present unless otherwise indicated, including:

a. Evidence concerning occupancy or ownership of [redacted] New Jersey 07010, a 2016 black Mercedes-Benz C300 bearing [redacted] and a 2021 white Mercedes-Benz GLE bearing [redacted] including utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, invoices, registration documents, identification documents, address books, and telephone directories.

b. Evidence concerning aliases or identities used by Oluwaseun ADEKOYA, including identification instruments and documents, financial records, telephone bills, legal records, and other documentation indicating the use by ADEKOYA of a name or identity other than ADEKOYA.

c. Evidence concerning the identity or location of, and communications with, suspects, coconspirators, and bank fraud or identity theft victims.

d. Records related to personal identifying information ("PII") of anyone other than ADEKOYA or his spouse, A[redacted] T[redacted] O[redacted]

e. Records related to credit unions or banks, to include locations, account numbers, participation in shared branching, shared branching transaction limitations.

f. Records related to fraudulent banking transactions conducted in the name of customers, including location information, branch information, transaction amounts, identity of individuals conducting the transactions or in whose name the transactions were conducted, and time and date of transaction.

g. Any and all financial and wealth information for ADEKOYA, including but not limited to bank account records, bank statements, deposit slips, ATM withdrawal slips, cancelled checks, check registers, withdrawal slips, wire and inter-account transfers, cryptocurrency transfers, cashier's checks, money orders, signature cards, mutual fund and other securities records, credit applications, loan documents and loan payments records, debit cards, credit cards, credit card statements, credit card account applications, invoices, vendor

payments, subcontractor invoices, insurance records, deeds, titles, receipts and/or bills evidencing cash expenditures.

h. Records related to the acquisition or purchase of customer financial information, PII, and fake identifications.

i. Evidence of the disposition of proceeds of the Subject Offenses, including U.S. currency, foreign currency, cryptocurrency, jewelry, precious metals, other valuables, pre-paid debit cards, financial instruments, and financial accounts constituting or traceable to the proceeds of the Subject Offenses, and including any passwords, passphrases, public or private keys, physical devices, physical keys, and cryptocurrency recover mnemonics needed by law enforcement to access such items.

j. Records and communications relating to the storage of items, records or documents at any other location, including but not limited to contracts and lease agreements for offices, storage units or safe deposit boxes. Keys and other access devices for storage units, safe deposit boxes, vehicles, and other closed containers.

k. Photographs and communications related to the crimes under investigation and identifying victims, coconspirators, or other evidence of criminal activity.

2. The items to be seized include any computer devices, cellular phones, and storage media reasonably believed to contain any electronically

stored information falling within the categories set forth in this Attachment B-3 above, including, but not limited to, desktop and laptop computers, tablets, disk drives, thumb drives, personal digital assistants, cellular phones, digital cameras, and portable scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review. The items to be seized include any cellular telephones that belong to ADEKOYA or are reasonably believed to have been used by ADEKOYA in connection with the Subject Offenses.

3. For any computer or storage medium, to include desktop and laptop computers, tablets, disk drives, modems, thumb drives, personal digital assistants, cellular phones, digital cameras, and scanners, whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or

absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and

cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

5. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

6. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

7. During the execution of the search, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of ADEKOYA to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face of ADEKOYA and activate the facial recognition feature, for the

purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

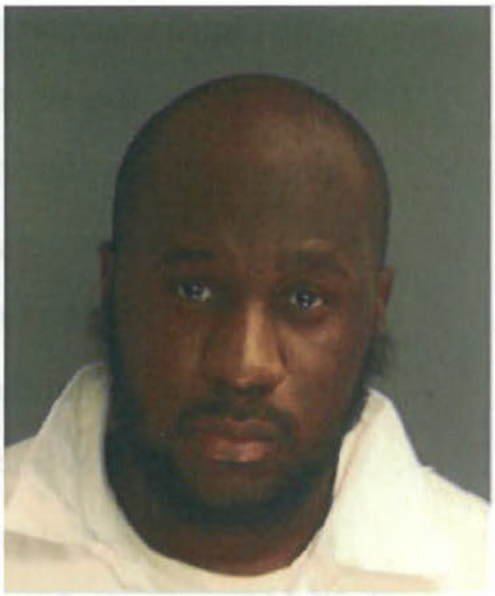
8. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT A-4

Person to be Searched

1. This warrant authorizes the search of the person of Oluwaseun ADEKOYA, date of birth, [redacted] wherever he is found within the District of New Jersey, as well as anything he is carrying or holding (e.g. backpack, bag, briefcase) when law enforcement encounters him. ADEKOYA is approximately 6 feet tall, weighing approximately 190 pounds. ADEKOYA has brown eyes, black hair, and a dark skin complexion. He is pictured below:

Surveillance photograph 7/17/23



Prison photograph approximately 2017

ATTACHMENT B-4

Items to be Seized

1. All evidence, fruits, and instrumentalities of the crimes of conspiracy to commit bank fraud, in violation of 18 U.S.C. §§ 1349 and 1344 and aggravated identity theft, in violation of 18 U.S.C. § 1028A (aggravated identity theft) (the "Subject Offenses"), involving Oluwaseun ADEKOYA and any co-conspirators known and unknown, covering the time period of January 1, 2021 to present unless otherwise indicated, including:

a. Evidence concerning occupancy or ownership of [redacted] New Jersey 07010, a 2016 black Mercedes-Benz C300 bearing [redacted] and a 2021 white Mercedes-Benz GLE bearing [redacted] including utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, invoices, registration documents, identification documents, address books, and telephone directories.

b. Evidence concerning aliases or identities used by Oluwaseun ADEKOYA, including identification instruments and documents, financial records, telephone bills, legal records, and other documentation indicating the use by ADEKOYA of a name or identity other than ADEKOYA.

c. Evidence concerning the identity or location of, and communications with, suspects, coconspirators, and bank fraud or identity theft victims.

d. Records related to personal identifying information ("PII") of anyone other than ADEKOYA or his spouse, A[redacted] T[redacted] O[redacted]

e. Records related to credit unions or banks, to include locations, account numbers, participation in shared branching, shared branching transaction limitations.

f. Records related to fraudulent banking transactions conducted in the name of customers, including location information, branch information, transaction amounts, identity of individuals conducting the transactions or in whose name the transactions were conducted, and time and date of transaction.

g. Any and all financial and wealth information for ADEKOYA, including but not limited to bank account records, bank statements, deposit slips, ATM withdrawal slips, cancelled checks, check registers, withdrawal slips, wire and inter-account transfers, cryptocurrency transfers, cashier's checks, money orders, signature cards, mutual fund and other securities records, credit applications, loan documents and loan payments records, debit cards, credit cards, credit card statements, credit card account applications, invoices, vendor

payments, subcontractor invoices, insurance records, deeds, titles, receipts and/or bills evidencing cash expenditures.

h. Records related to the acquisition or purchase of customer financial information, PII, and fake identifications.

i. Evidence of the disposition of proceeds of the Subject Offenses, including U.S. currency, foreign currency, cryptocurrency, jewelry, precious metals, other valuables, pre-paid debit cards, financial instruments, and financial accounts constituting or traceable to the proceeds of the Subject Offenses, and including any passwords, passphrases, public or private keys, physical devices, physical keys, and cryptocurrency recover mnemonics needed by law enforcement to access such items.

j. Records and communications relating to the storage of items, records or documents at any other location, including but not limited to contracts and lease agreements for offices, storage units or safe deposit boxes. Keys and other access devices for storage units, safe deposit boxes, vehicles, and other closed containers.

k. Photographs and communications related to the crimes under investigation and identifying victims, coconspirators, or other evidence of criminal activity.

2. The items to be seized include any computer devices, cellular phones, and storage media reasonably believed to contain any electronically

stored information falling within the categories set forth in this Attachment B-4 above, including, but not limited to, desktop and laptop computers, tablets, disk drives, thumb drives, personal digital assistants, cellular phones, digital cameras, and portable scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review. The items to be seized include any cellular telephones that belong to ADEKOYA or are reasonably believed to have been used by ADEKOYA in connection with the Subject Offenses.

3. For any computer or storage medium, to include desktop and laptop computers, tablets, disk drives, modems, thumb drives, personal digital assistants, cellular phones, digital cameras, and scanners, whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or

absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and

cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

5. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

6. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

7. During the execution of the search, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of ADEKOYA to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face of ADEKOYA and activate the facial recognition feature, for the

purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

8. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.